Sending Files to External Parties

Back to Practices Page

Practice

Electronic File transfers to External Parties must be conducted in a manner consistent with information security practices and policies.

Purpose

Information Assets shall be used for their intended purposes only, and must be protected when not in the possession of CalPERS.

This Practice is the final, definitive authority on the subject of Electronic File Transfers to External Parties, and supercedes and replaces any other Policies, Practices or Procedures, unless the Sending Files to External Parties Practice itself provides otherwise.

Definitions

Please check the Information Security Office's online Glossary for the definitions of additional terms not found in this document.

External Custodian	External Party using or storing CalPERS information assets as a result of contractual and /or other agreements.
External Custodian of Information Assets Practice	Information Security Practice that defines the responsibilities and requirements of an External Custodian. External Custodian of Information Assets Practice
Information Asset	Any hardware, software or network components that contain or are used to process, manage or store information necessary to the operation of CalPERS. In addition all data, including electronic files and records, and that found on paper or other storage media.
Storage Media	Any of a number of devices used to store data, including but not limited to, hard disk drives, diskettes, USB drives, CDs, DVDs and tape.
Media Transport Practice	Information Security Practice that defines the requirements for the use of media when transporting CalPERS information assets. Media Transport Practice

Sending Files to External Parties

Back to Practices Page

Production Operations File Transfers

For the purposes of this Practice, Electronic File Transfers out of CalPERS that support ongoing functions necessary for CalPERS to meet its obligations and commitments to members, employers and business partners. There are three types of Production Operations File Transfers:

- Automated and Unattended
- On-Demand
- System Support

Automated and Unattended Production Operations File Transfer

Production operation processes that are triggered by an automated scheduler to run on a pre-defined date using consistent selection criteria. These processes run without any intervention by IT staff whatsoever other than to start the automated process; they require no changes to the data selection criteria (e.g., monthly retirement roll, transmission of enrollment and health claim data to health carriers, transmission of CalPERS payroll information to the State Controller).

On-Demand Production Operations File Transfer

A pre-defined file or report containing pre-defined data elements is created based on specific selection criteria that are provided and submitted. These files can be created by either ITSB staff or by Program staff using applications developed for this purpose.

System Support Production Operations File Transfer

Files created by a system in response to unexpected conditions that cause normal processing to fail, and facilitate troubleshooting and defect resolution.

Ad-Hoc File Transfer

File transfers that are done a single time for a specific purpose.

Personal Information	Personal information is information in CalPERS' possession that describes or identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Examples of personal information include, but are not limited to, five or more numbers in sequence of a social security number; first or last name; physical description; physical address(es); home, mobile, cellular, two-way radio or fax number(s); e-mail, web site, or social networking address(es); educational information including schools attended, level of education or degrees earned; financial information including federal and state tax information or account or contract number of a financial institution(s); marital or domestic partner status; medical information including past, present, or future physical or mental health diagnosis or treatment, insurance policy or subscriber numbers, applications for insurance, claims histories or appeals; past, present or future place of employment or employment status; name of attorney, guardian/conservator, or power-of-attorney; video or voice recordings or pictures; and statements made by, or attributed to, the individual, in any form. The list included with this definition is not intended to be exhaustive of every type of information in CalPERS possession that is personal information.
Receiving Party	Any External Party that receives data from CalPERS
External Party	An entity outside of CalPERS.
Quality Control Measures	Any of a number of processes or functions established to ensure accuracy and integrity of information. For On-Demand, System Support and Ad-Hoc File Transfers, at minimum an approved SEIA must be on file with the ISOF and a completed SFTCL must be approved by and filed with the Data Owner prior to transfer of data outside of CalPERS.
Requestor	In the context of this Practice, a Requestor is a CalPERS program unit that requests information be sent to a receiving party.
Internal Data Custodian	The CalPERS unit with the authority and responsibility to manage Information Assets. This includes responsibility to ensure the accessibility, integrity and security of information assets. In most cases, ITSB is the Internal Data Custodian.
CalPERS Data Custodian	This is another designation sometimes used to refer to the entity within CalPERS with custodial responsibilities for Information Assets. See *Internal Data Custodian*.

NDA	Non-Disclosure Agreement Form See also the Non-Disclosure Practice .
SEIA	Sending Electronic Information Agreement Form. This is the form used to document the transfer of information outside of CalPERS and must be completed prior to the initial run of every Automated and Unattended Production Operations File Transfers, On Demand Production Operations File Transfers, System Support Production Operations File Transfers, and Ad-Hoc File Transfers.
SEIA-NP	Sending Electronic Information Agreement Form - Non-Personal This is the form used to document electronic file transfers when the systems from which data are extracted for transfer do not contain any personal information.
SFTCL	Sending File Transfer Check List . This is the form that must be completed for each instance of an On Demand and System Support Production Operations and Ad-Hoc File Transfers
Data Owner	An individual that classifies and secures information assets for which they are responsible.
Data Owner and Custodians Practice	Information Security Practice that defines the responsibilities of CalPERS data owners and custodians. Data Owners and Custodians Practice
Sender	In the context of this Practice, the individual who transmits a file in whatever form the transmittal takes, including email, FTP, or mailing of storage media.
Processor	In the context of this Practice, the organizational unit or individual who prepares a file for transmittal.
Information Security Incident	A successful security event that has caused the unauthorized disclosure, modification, destruction or misuse of a CalPERS information asset. The CalPERS Information Security Office has an electronic Information Security Incident Report form for reporting security incidents.

Information Security Incidents Practice	Information Security Practice that defines requirements pertaining to the reporting of security incidents. Information Security Incidents Practice
Information Security Event	An attempted unauthorized access, use, disclosure, modification or destruction of information or interference with systems operations in an information system. Examples include, but are not limited to, pings on a firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, or malware (e.g. worms, viruses).
Incident Handling	An action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used by unintended recipients.
Encryption of Electronic Communications	Information Security Practice that defines the requirements for the use of encryption in CalPERS. Encryption of Electronic Communications Practice
Critical application	Those applications identified in the Business Continuity Plan as essential and critical to the continued function of CalPERS

Requirements

General Requirement	
Approval - SEIA	All Electronic File Transfers require an approved SEIA form, (Sending Electronic Information Agreement Form), including Automated and Unattended, On-Demand and System Support Production Operations File Transfers, and Ad-Hoc File Transfers. The completed SEIA must be signed by the Data Owner, the applicable CalPERS AEO, the CalPERS Data Custodian, and the Receiving Party.
Approval - SEIA-NP	If the system(s) from which data are extracted for an Electronic File Transfer do not contain any personal information, the SEIA-NP form may be used.

SFTCL	Every instance of On-Demand and System Support Production Operations File Transfers and Ad-Hoc File Transfers authorized with a SEIA requires an SFTCL. Exemption from this requirement for file transfers authorized with a SEIA-NP may be requested from the ISOF.
Encryption	All Information Assets transferred by CalPERS to receiving parties must be encrypted in accordance with ISOF encryption practice Encryption of Electronic Communications Practice. Encryption methodology is identified on the SFTCL and is approved in advance of the file transfer by the ISOF.
Requesting ITSB to transfer data files	ITSB will process a request to transmit data only upon receipt of a Service Request and only after a SEIA for the requested file transfer has been approved by the appropriate AEO and the ISOF.
Quality Control	An SFTCL must be completed prior to transmittal of On-Demand or System Support Production File Transfers or for Ad-Hoc File Transfers for all File Transfers authorized with an SEIA. The Data Owner, Processor, Requestor and Sender must all validate accuracy of the contents of a file to be transmitted on the SFTCL.
Data Owner Responsibilities	Data owners must review all requested Electronic File Transfers and ensure they are necessary for legitimate business purposes. Data owners must authorize each instance of On-Demand File, System Support or Ad Hoc Transfers with SFTCLs. Any change to the data description, means of transmittal, destination or transmittal schedule must be approved on an amended SEIA Data Owner must sign SEIAs and SEIA-NPs under the *Affirmation Statement of CalPERS Data Owner*, validating the completeness of information and business need for the File Transfer
Requestor Responsibilities - SEIA	Requestor must describe, in detail, in the SEIA the reason for the Electronic File Transfers. Requestor must include a list of all data elements to be included in the Electronic File Transfers, and identify those that include Personal Information Requestor must identify the receiving party to whom Information Assets are to be Electronically Transferred.

Requestor must identify how long receiving parties shall retain the data sent to them. The default period is 30 days, unless otherwise specified in the SEIA.

Requestor must ensure that certification of destruction is provided by the Receiving Party within 5 working days following the date by which the data must be destroyed.

Requestor must identify the means of transferring the file.

Requestor must provide a signed NDA (Non-Disclosure Agreement form) from the Receiving Party unless the Receiving Party has a contractual relationship with CalPERS where confidentiality language equivalent to that in the NDA is in place, in which case, the contract number and copies of the relevant contract sections must be provided to the ISOF when the SEIA is submitted.

Requestor must obtain the signature of a legal representative of the Receiving Party in the SEIA section, *Affirmation Statement of the Receiving Party,* unless the Receiving Party has a contractual relationship with CalPERS and equivalent data custodian responsibilities have been defined in the contract, in which case the data owner must provide the contract number and copies of the relevant contract sections to the ISOF when the SEIA is submitted.

Requestor Responsibilities – SEIA-NP

Requestor must describe, in detail, in the SEIA-NP the reason for the Electronic File Transfers

Requestor must provide a list of all data elements included the system(s) from which data are extracted for the requested File Transfer.

Requestor must identify the Receiving Party to whom Information Assets are to be Electronically Transferred.

Requestor must identify how long receiving parties shall retain the data sent to them. The default period is 3 days.

Requestor must identify the means of transferring the file.

Requestor must provide a copy of the contract or reference to the contract that defines the relationship between CalPERS and the Receiving Party that gives rise to the need for the File Transfer.

	Requestor must affirm that disclosure of the data elements in the system(s) from which the data are extracted will not result in a breach of contract between CalPERS and any third party.
Requestor Responsibilities – SFTCL	Requestors must complete their sections of the SFTCL for each instance of an authorized file transfer, including validation that the file prepared for transmittal contains only the data requested for transmittal. Requestors must obtain authorization from Data Owner prior to submitting a Service Request to ITSB to request a file transfer.
Processor Responsibility	Processors must complete their section of the SFTCL for each requested Electronic File Transfer, including validation that the file prepared for transmittal contains only the data requested for transmittal.
Sender Responsibility	Senders must complete their section of the SFTCL for each file transfer, including validation that transmittal method and encryption process used are consistent with the SFTCL, and receiving party address to which the file is sent matches the address provided in the SFTCL.
AEO Responsibilities	All SEIAs and SEIA-NPs must be approved by the appropriate AEO. AEO signature is required on all SEIAs and SEIA-NPs. AEO attests that there is a necessary and legitimate business purpose for the requested file transfer by signing the AEO Affirmation Statement in the SEIA.
Internal Data Custodian Responsibilities	Internal Data Custodian shall process On-Demand File or System Support Production File Transfers or Ad-Hoc File Transfers after they receive a completed Service Request and a completed SFTCL. Internal Data Custodian must identify the systems or applications from which files for transfer are made. System Support File Transfers must have approved SEIAs on file with the ISOF prior to any file transfer being made. An SFTCL must be completed for each instance of a System Support File Transfer Processing of Unattended File Transfers must conform to that described in the SEIA or SEIA-NP.

ISOF Responsibilities	ISOF shall review and ensure completeness of all SEIAs and SEIA-NPs, including signatures in all Affirmation Statement sections.
	ISOF ensures that no personal information data elements are present in any of the systems from which data may be extracted for inclusion in File Transfers authorized with a SEIA-NP.
	ISOF reviews SEIAs and SEIA-NPs to ensure consistency between the Description and Purpose sections.
	ISOF maintains copies of SEIAs, SEIA-NPs completed SFTCLs for all file transfers.
	ISOF reviews requests for exemptions from SFTCL requirement for On-Demand, System Support and Ad Hoc File Transfers authorized with a SEIA-NP.
	ISOF forwards informational copies of completed SEIAs and SEIA-NPs to ITSB.

Compliance

Compliance Measurement	ISOF will periodically measure compliance with this Practice.
Incident Handling	If an individual within CalPERS suspects or knows of an unauthorized transmittal of information, even as a result of an accident or mistake, the incident must be reported to the ISOF immediately, in accordance with the Information Security Incidents Practice.
Incident Handling	ISOF will notify General Counsel, Division/Office Chief and AEO of the possible incident as soon as possible, but no later than 24 hours
Incident Handling	ISOF will conduct an investigation of the incident and prepare an incident report, in accordance with the Information Security Incidents Practice (http://insider.calpers.ca.gov/isof/sub/practices/Information-Security-Incidents.pdf).
Disciplinary Action	Refer to the, CalPERS Information Security Policy, Information Security Compliance.

Employees who fail to comply with security policies and procedures may be subject to sanctions, including dismissal, demotion, suspension, or other disciplinary action pursuant to provisions set forth in Government Code section 19572 et. seq.

Contractors, consultants or students who fail to comply with security policies and procedures may be subject to sanctions including termination of their contract.

Authority

CalPERS Information Security Policy

Revisions

Effective: February 7, 2008